SAP Security Overview

Shelly Eckerman
Security Lead
Bearing Point

BEACON

Purpose of Meeting

- To gain an understanding of SAP Security Concepts
- To gain an understanding of how SAP Security is designed and configured
- To explain the SAP Security thread within the ProvenCourse methodology
- To discuss how the Security Team will work with the teams during blueprint to collect security information

Project/Support Teams versus End Users

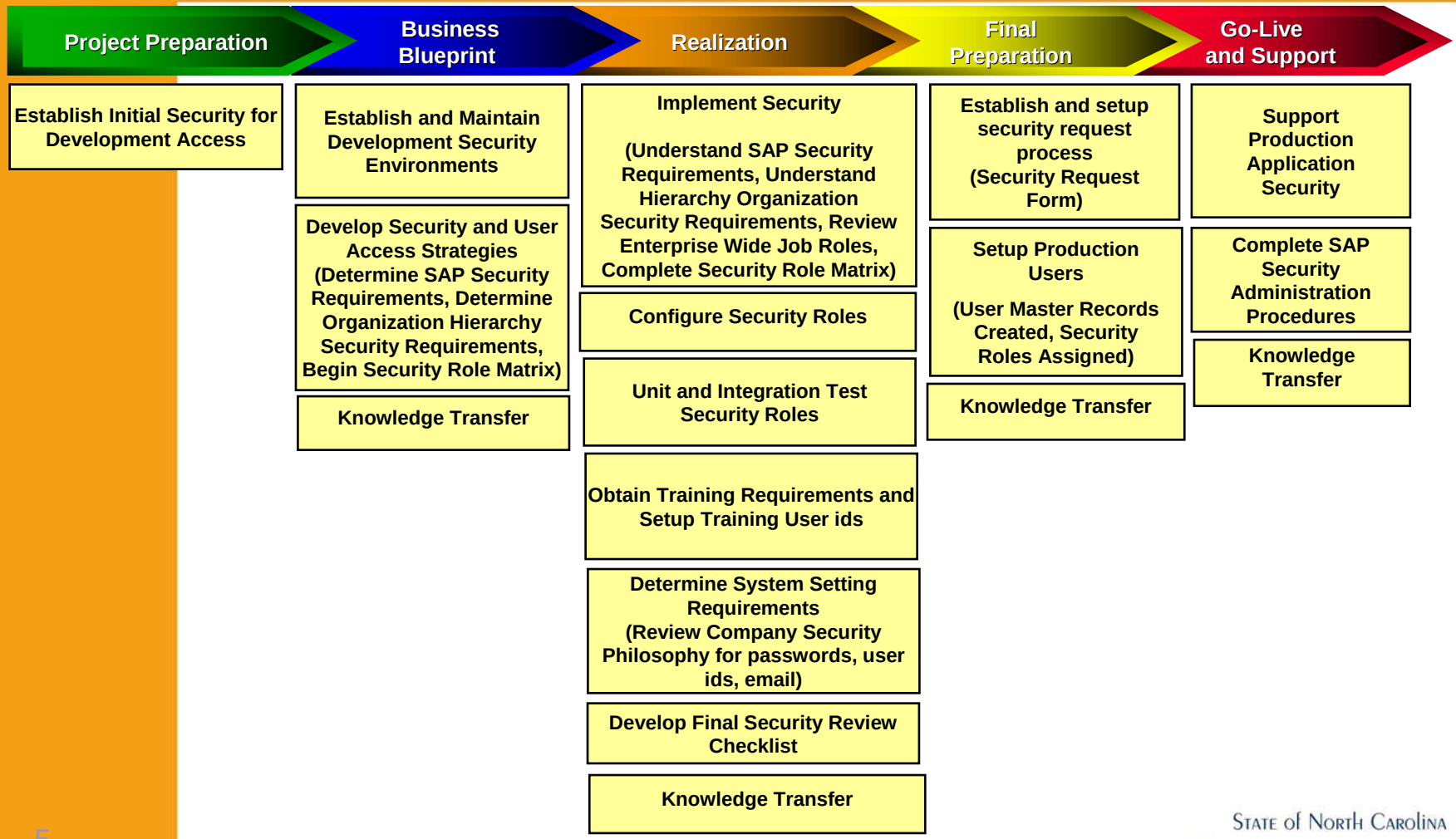
- Different Types of Users
  - Project/Support Teams
    - These are the Basis, ABAP programmers, Functional Configuration teams
    - Project Teams and Support Team user access for Production will be designed by the security team closer to go-live. Not critical for integration testing
  - End users
    - These are the users that will have access in production via the portal and R/3 from the agencies
    - End User Access Requirements are what the security team will focus on designing and configuring for integration testing
    - This is also the focus for this presentation

BEACON

About ProvenCourse Methodology

- The ProvenCourse methodology is based on a 'Roadmap' concept. The Roadmap acts as a guide for the project, specifying steps, identifying milestones, and setting the pace for the entire project.
- The Roadmap consists of five phases:
  - Phase 1: Project Preparation (initial scoping/planning)
  - Phase 2: Business Blueprint (data gathering)
  - Phase 3: Realization (configuration and testing)
  - Phase 4: Final Preparation (training and cut-over)
  - Phase 5: Go-Live and Support (actual go-live)

ProvenCourse for SAP Security



Implementing SAP Security

Building the Security Role Matrix

- Transaction codes in scope for R/3, including the Portal
- Infotypes in scope, including the Portal
- Security Roles Defined

Security Role Matrix Example

Transactions		HR Organization Maintenance	HR Organization Display	HR Pay Maintenance	HR Pay Display	HR Administration Maintenance	HR Administration Display
HR MASTER DATA							
PA10	Personnel File			X			
PA20	HR Master Display			X			
PA30	HR Master Update			X			
PA40	Personnel Actions			X			
PA42	Fast Entry: Actions			X			
PA70	Fast Entry			X			
HR ADHOC QUERY							
S_PH0_48000513	Ad Hoc Query						
S_PH0_48000510	Ad Hoc Query						
ORGANIZATIONAL MANAGEMENT							
OODT	Transfer of Legacy Data	X					
OOHQ	Integration PA	X					
OOMV	Create Sequential File	X					
PFAL	Distribute Master Data	X					
PFCT	Expert Mode - Task Catalog	X					

P_Orgin	HR Master Data Infotypes	HR Organization Maintenance	HR Organization Display	HR Pay Maintenance	HR Pay Display	HR Administration Maintenance	HR Administration Display
R	**Matchcode/Read Access**						
W	**Write Access**						
0000	Actions					W	R
0001	Organizational Assignment					W	R
0002	Personal Data					W	R
0003	Payroll Status					W	R
0004	Challenge					W	R
0005	Leave Entitlement					W	R
0006	Addresses					W	R
0007	Planned Working Time					W	R
0008	Basic Pay			W	R		
0014	Recurring Payments/Deductions			W	R		
0015	Additional Payments			W	R		
0009	Bank Details			W	R		
0010	Capital Formation					W	R

Implementing SAP Security

- Understanding Agency Restrictions
  - Hierarchy Organization Security Requirements
  - What data should and should not be viewed across agencies
  - What data should be restricted within an agency

NOTE:

Naming Conventions are Important!!

EXAMPLE

SECURITY HIERARCHIES	Personnel Area	Employee Group	Employee Subgroup	HR Plan version	Payroll Area	Time Data Entry Profile	Controlling area	Cost Center	Profit Center	Order Type	Cost Element	Company Code	Chart of Accounts	Office (Business Area)	Vendor Acct Grp	Vendor Auth Grp
	PERSA	PERSG	PERSK	PLVAR	ABRKS	n/a	KOKRS	KOSTL	PRCTR	AUFART	KSTAR	BUKRS	KTOPL	GSBER	KTOKK	BRGRU
AR (Argentina)	AR*	*	*	01	AR	ZAR*	1001	AR*	AR*	AR*	*	AR*	ARCA	AR*	AR*	AR*
CR (Costa Rica)	CR*	*	*	01	CR	ZCR*	1004	CR*	CR*	CR*	*	CR*	CRCA	CR*	CR*	CR*
GT (Guatemala)	GT*	*	*	01	GT	ZGT*	1006	GT*	GT*	GT*	*	GT*	GTCA	GT*	GT*	GT*
NI (Nicaragua)	NI*	*	*	01	NI	ZNI*	1003	NI*	NI*	NI*	*	NI*	NICA	NI*	NI*	NI*
PA (Panama)	PA*	*	*	01	PA	ZPA*	1005	PA*	PA*	PA*	*	PA*	PACA	PA*	PA*	PA*
PY (Paraguay)	PY*	*	*	01	PY	ZPY*	1008	PY*	PY*	PY*	*	PY*	PYCA	PY*	PY*	PY*
UY (Uruguay)	UY*	*	*	01	UY	ZUY*	1002	UY*	UY*	UY*	*	UY*	UYCA	UY*	UY*	UY*
VE (Venezuela)	VE*	*	*	01	VE	ZVE*	1007	VE*	VE*	VE*	*	VE*	VECA	VE*	VE*	VE*
EQ (Ecuador)	EQ*	*	*	01	LB	ZEQ*	1009	EQ*	EQ*	EQ*	*	EQ*	?????	EQ*	EQ*	EQ*
PE (Peru)	PE*	*	*	01	PE	ZPE*	1010	PE*	PE*	PE*	*	PE*	CAPE	PE*	PE*	PE*

Implementing SAP Security

- Role to Position to User Mapping
  - Security will work with the Change team for “role to position to user mapping”
  - Security will use the mapping to complete the security design

SAP Application Security Construct

SAP Transaction(s) & Infotypes

Simple Role(s) "Pay Maintenance"

Composite Security Roles (Job or Position) "Payroll Clerk"

- Simple Roles are functions done in SAP.
- Two Groups of Simple Roles
  - Simple Roles consistent across organization
  - Simple Roles that include the differences of an agency
- A Position will have many simple roles

SAP application security is "*Role Based*" – Simple Roles are job functions mapped to positions which are mapped to users. It allows users to be given access based on their job responsibilities.

Position Based Security

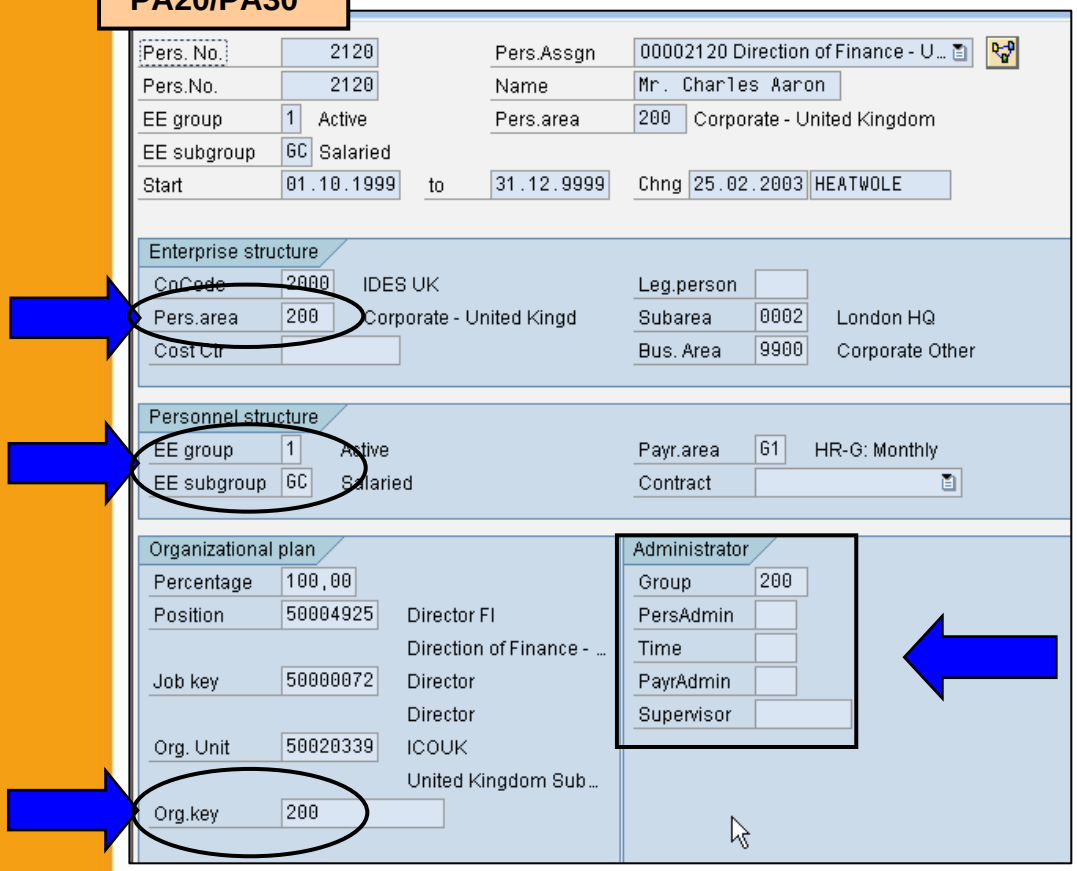
- Position Based
  - When a person is hired into the organization, the user id is automatically created
  - Access assigned is based on roles assigned to position
  - Manual access can also be granted
    - Person transfers to another position, but still requires access to old positions access

HR Security

- Standard HR Security
  - Security on the HR Master Data
    - Personnel Area
    - Employee Group
    - Employee SubGroup
    - Organization Key
    - Admin Groups
- Structural HR Security
  - Security on the Organization Structure

HR Standard Security

PA20/PA30



Personnel Area

- Secured by each agency

Employee Group

Employee Sub Group

Org Key

- Fields within PA20/PA30 can be added to the org key, then we can secure on the Org Key
- Important to use Org Key for security

Administrator

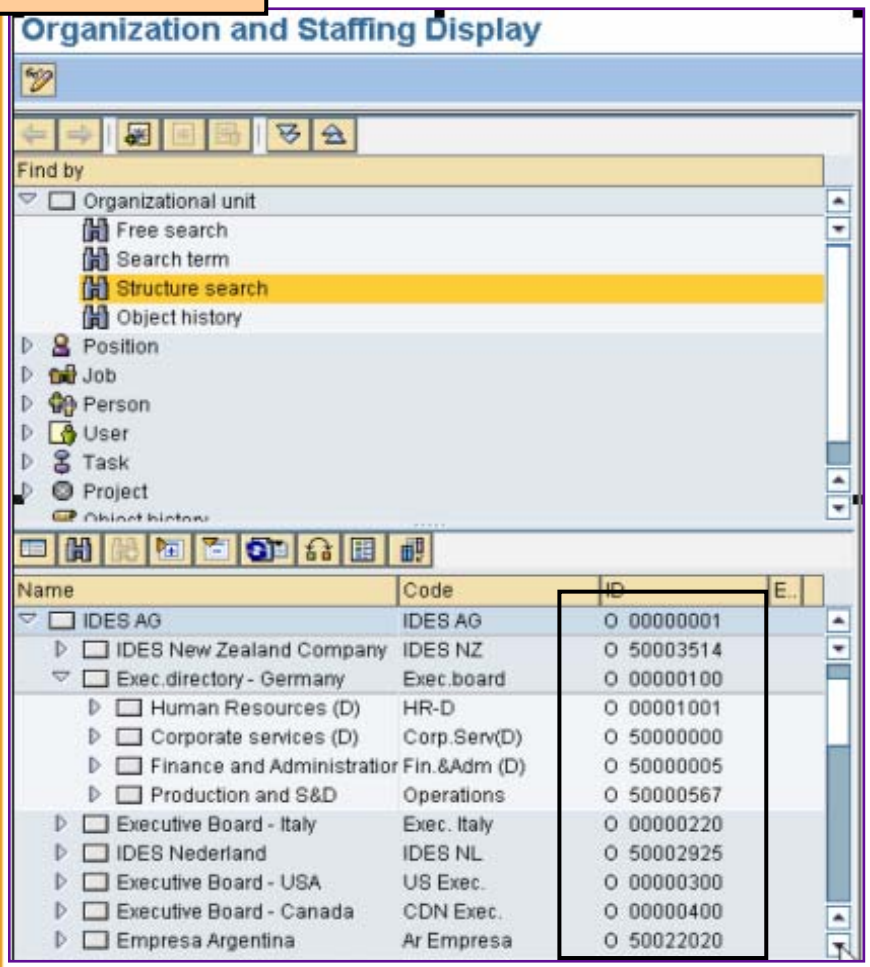
- Able to secure on these groupings

NOTE: ESS/MSS Portal

- Security on backend works the same

HR Structural Security - Organization

PPOSE/PPOME

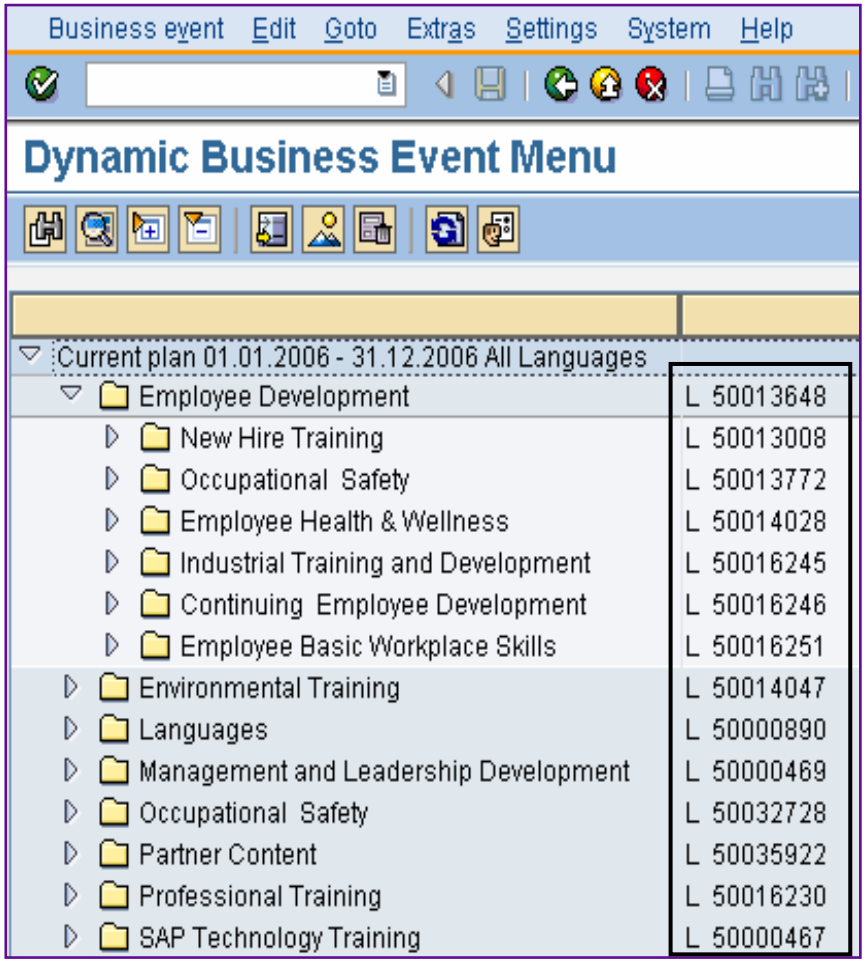


Structural Security

- Allows to secure by a structure
- For the Org Structure, security is built on the Org Unit

HR Structural Security – Training & Events

PSV2



Structural Security

- Allows to secure by a structure
- For Training & Events, security is built on Course Group

Other HR Security Levels

- Time Management
  - Data Entry Profile
- Payroll
  - Payroll Area
- HR Organization
  - HR Plan Version
- HR Personnel Administration
  - HR Infotypes

Key FI/CO Security

- Finance Security
  - Company Code
  - Business Area
  - Funds Center
  - Document Type
  - Vendor Account Group
  - Vendor Authorization Group (can be enabled)
- Controlling
  - Controlling Area
  - Cost Center
  - Cost Element
  - Profit Center

Internal Controls

- Segregation of Duties (SOD)
  - SOD Analysis will be reviewed
  - Security is configured based on SOD Requirements
  - SOD is not as widely required in HR
- Key HR Control
  - Restricting Users from being able to update their own information (i.e. Salary)
  - Restricting Users to only being able to update their own information (i.e. Timesheet entry)

Technical Security

- Access to Tables
  - End Users will not get access to SE16, SE16n, SE17, SM30 or SM31
  - Risk: when updating or viewing a table, security is not restricted at the hierarchy organization level (i.e. Personnel Area, etc)
  - If access to a table is required for an end user and it is okay they see all data in the table, a custom transaction code should be created. Access to the custom transaction would be assigned to the role.

BEACON

Technical Security

- Access to Programs
  - End Users will not get access to SE38 or SA38
  - Risk: SE38/SA38 is a backdoor to running a transaction. User could be running a program the project team did not want run
  - All programs need to be run via a transaction code. If the program does not have a standard SAP transaction code assigned, then a custom transaction code should be assigned. Access to the custom transaction would be assigned to the role.

Technical Security

- Access to SAP Spools
  - End Users will have access to see their own spools, but not other user's spool
  - If there is a spool a user is required to see, then batch ids will be setup and the program should be scheduled under the batch id. Access to the batch id would be added the security role.
  - Note: if batch ids are required, it must be considered if a different batch id is required for each agency.

Testing

- Development
  - Unit Testing occurs in development system
  - Teams have full functional (all HR, all FI/CO) access
  - Also, in the development system, we will setup security test ids so we can begin testing security (especially Portal) and are also useful to understand how security will work for our end users
  - Security may need a couple day turn around for decisions to be validated and security fixed during the stage where dev is used
- QA
  - Security is tested during Integration Testing/UAT in the QA system
  - Test ids will equal a security role
  - Test ids are used to test the transaction scenarios
  - Security will be sitting in the Integration Testing Room and any authorization problems that are encountered are fixed immediately
    - It is normal to have security problems during integration testing
    - Integration testing is the place to fix the issues
    - If security is not tested, then many issues at go-live

Authorization Issues

- During the project and integration testing, you may get a no authorization message
- Anytime the no authorization message appears, then immediately go to the command line and type /nsu53
- The security team needs the su53 report and to know which transaction code you were in when you got the no authorization message

Security Team

- Security Decisions
  - As workshops are going on for blueprint, please contact the security team if you have any questions on how something needs to be secured
  - We can attend any workshops that would be useful for us to obtain our security requirements and so we are there to answer how security can be secured

- Security Team
  - Shelly Eckerman – Security Lead (BP)
  - TBD – IT Security Lead (OSC)
  - TBD – Security Consultant (BP)
  - TBD – IT Security Analyst (OSC)